# The evolving landscape of cybersecurity in 2024



In 2024, the cybersecurity landscape witnessed a considerable increase in high-profile cyber attacks across various sectors, highlighting the significant vulnerabilities businesses face in today’s interconnected world. The global annual cost attributed to cybercrime damage is projected to reach $10.5 trillion, as reported by Cybersecurity Ventures. Industries heavily affected included healthcare, telecommunications, finance, and governmental services, with critical infrastructure and sensitive data representations at risk amid sophisticated attacks such as ransomware and supply chain breaches.

Notably, cybercriminal groups such as ALPHV/BlackCat and Termite were responsible for prominent ransomware incidents. A crucial trend observed was the targeting of supply chains, whereby attackers exploited third-party vulnerabilities to infiltrate multiple organisations simultaneously. Key incidents included the breach of the U.S. Cybersecurity and Infrastructure Security Agency (CISA) due to vulnerabilities in Ivanti VPN software and a SIM-swapping attack against the U.S. Securities and Exchange Commission (SEC), demonstrating the diversity and complexity of cyber threats faced by organisations.

The incident involving CISA was of particular significance, occurring in early 2024. The breach was related to several flaws in Ivanti's products that allowed attackers to remotely access key systems essential to monitoring critical infrastructure. It highlighted a dramatic risk stemming from third-party dependencies, leading to immediate remedial actions taken by CISA, including the disconnection of federal agencies from affected systems.

Similarly, the SEC’s experienced vulnerability to SIM-swapping underscores the disruptive potential of these attacks. An attacker managed to hijack the SEC's phone number and disseminate false information regarding Bitcoin Exchange-Traded Funds (ETFs), leading to significant market impacts. The increase in SIM swapping cases—exceeding 800 throughout 2024—demonstrates the mounting risks not just for individuals but for institutions as well.

The healthcare sector, handling sensitive patient data, faced considerable breaches in 2024. A significant ransomware attack on Change Healthcare disrupted service for over ten days and raised concerns regarding further data breaches linked to its partners. Another major breach occurred at Cencora Healthcare, compromising patient data from several leading pharmaceutical companies, while HealthEquity reported a breach impacting 4.3 million individuals due to a vendor’s compromised account. These incidents reinforced the need for heightened third-party risk management practices and robust data protection strategies in the healthcare industry.

The financial sector also experienced serious challenges, most prominently illustrated in the attack on Financial Business and Consumer Solutions (FBCS), where sensitive data of over four million individuals was exposed. The breach, affecting clients such as Comcast and Truist Bank, prompted discussions around the responsibilities businesses hold in ensuring robust security measures when engaging with third-party vendors.

Moreover, in May 2024, a substantial data breach involving the cloud data platform Snowflake was uncovered, with sensitive data from high-profile clients including Santander Bank and Ticketmaster being compromised. Attackers exploited weak security protocols, revealing the urgent need for improved credential security and resilient cloud configurations.

Following these significant incidents, experts are emphasising critical lessons for businesses to integrate into their cybersecurity strategies moving forward. Key recommendations include embracing advanced threat intelligence solutions, regularly patching vulnerabilities in both internal and third-party software, and maintaining continuous monitoring and robust incident response plans. Furthermore, with businesses increasingly turning to machine learning operations (MLOps) for their AI deployment, security measures must become paramount. Understanding the potential attack vectors against MLOps platforms could mitigate risks associated with data poisoning and model extraction, recognising that attackers see these platforms as attractive targets given their growing prominence.

As we move into 2025, it is clear that organisations across industries must prioritise their cybersecurity posture, not only by bolstering existing frameworks but also by adapting to emerging technologies and vulnerabilities inherent in their supply chains and operational frameworks. SOCRadar’s offerings, such as its Extended Threat Intelligence (XTI) platform and Vulnerability Intelligence module, provide solutions aimed to enhance the visibility and defence capabilities against the ever-evolving landscape of cyber threats.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://nordlayer.com/blog/cybersecurity-statistics-of-2024/> - Corroborates the increase in cyber attacks, ransomware, and data breaches in 2024, including the targeting of telecommunications and healthcare sectors.
2. <https://www.cm-alliance.com/cybersecurity-blog/december-2024-major-cyber-attacks-data-breaches-ransomware-attacks> - Provides details on significant cyber attacks and data breaches in December 2024, affecting various sectors including healthcare and telecommunications.
3. <https://nordlayer.com/blog/cybersecurity-statistics-of-2024/> - Mentions the National Public Data breach and the attack on Change Healthcare, highlighting the severity of data breaches in 2024.
4. <https://www.cm-alliance.com/cybersecurity-blog/december-2024-major-cyber-attacks-data-breaches-ransomware-attacks> - Details the breach at ConnectOnCall and Texas Tech University, emphasizing the impact on healthcare and educational institutions.
5. <https://nordlayer.com/blog/cybersecurity-statistics-of-2024/> - Discusses the Chinese hacking campaign 'Salt Typhoon' targeting U.S. telecom companies, including Verizon, AT&T, and T-Mobile.
6. <https://www.cm-alliance.com/cybersecurity-blog/december-2024-major-cyber-attacks-data-breaches-ransomware-attacks> - Mentions the breach at American Addiction Centers and HealthEquity, highlighting the vulnerabilities in the healthcare sector.
7. <https://www.cm-alliance.com/cybersecurity-blog/december-2024-major-cyber-attacks-data-breaches-ransomware-attacks> - Reports on the breach involving the cloud data platform Snowflake, affecting clients like Santander Bank and Ticketmaster.
8. <https://nordlayer.com/blog/cybersecurity-statistics-of-2024/> - Highlights the surge in DDoS attacks and ransomware incidents, including the significant increase in daily cyber threats tracked by Amazon.
9. <https://www.cm-alliance.com/cybersecurity-blog/december-2024-major-cyber-attacks-data-breaches-ransomware-attacks> - Details the impact of SIM-swapping attacks, such as the one against the U.S. Securities and Exchange Commission (SEC).
10. <https://nordlayer.com/blog/cybersecurity-statistics-of-2024/> - Corroborates the targeting of supply chains and third-party vulnerabilities, such as the breach related to Ivanti VPN software affecting CISA.
11. <https://www.cm-alliance.com/cybersecurity-blog/december-2024-major-cyber-attacks-data-breaches-ransomware-attacks> - Emphasizes the need for robust security measures and continuous monitoring in light of the evolving cyber threat landscape.
12. <https://news.google.com/rss/articles/CBMikwFBVV95cUxNQlhrX3Q4U3lCMnhPdURha2kyUS1XTW1RemtzVExpczh4dERIUloyUHhLeTFEdEs1WVdxOS14MVVLNF9nNVNvWXhMZC1Da0ExaW9oT2dDdUdDaUVTTmp1UURUSFc3RkxjSlpsR1ZPVEpqM3RoeU5WMGlxTDl0bmxGOGpDTFNraUpZWDN6SWpGM1RuSDQ?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data
13. <https://news.google.com/rss/articles/CBMisAFBVV95cUxOMm41dTZ1dHRnaEFMVmh0a2VpczVwY3BoMl83dHFTOUVlalIzSU5lU1laSnEtWkhUV2xOcHBOTUZkRmlmeUJGYnNMUzlBaU1BTnl0RmVRSVJCcVJGUVRJWHM4cHJRTEZNdGlwSnRKZmtVZlpyWWFoel9uYzZuV1BaNkk1Z1FwQkFWdS1nUFM4VUtVRFloX2dzZk9LRXFLYW9zMnNuZTU3RGtkQmlMNmljeA?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data